How medium sized mammals defend our network!

Tim Clark (eclipse)

November 1, 2011

IPSec

- Secure tunnels over IP
- Uses racoon
- Needs setkey
- Usually auth with shared keys
- Can auth with public keys (X.509)

Racoon

- The thing you need to do IP tunnels
- IKE Daemon
- IKE=Internet Key Exchange
- Negotiates keys to make a IPSec tunnel
- IPSec tunnels use ESP (seriously)
- ESP=Encapsulating Security Payload

Setkey

- Causes the tunnel to be used
- Sets the security policy
- For example: when talking to SUCS only talk through the tunnel, and only listen to SUCS if its through the tunnel
- The tunnel doesn't exist till its needed
- Setkey is the thing that tells racoon to make the tunnel

Racoon

```
path pre_shared_key "/etc/racoon/psk.txt";

remote 137.44.6.5 {
        proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method pre_shared_key;
                dh_group modp1024;
        }
        lifetime time 60 min;
        exchange_mode main;
}
```

Racoon

```
sainfo
  address 137.44.10.0/24[any] any
  address 137.44.6.5[any] any {
        pfs_group modp1024;
        lifetime time 20 min;
        encryption_algorithm 3des;
        authentication_algorithm hmac_sha1;
        compression_algorithm deflate;
}
```

Setkey

```
spdadd 137.44.10.0/24 137.44.6.5 any -P out ipsec
    esp/tunnel/137.44.19.200-137.44.6.5/require;

spdadd 137.44.6.5 137.44.10.0/24 any -P in ipsec
    esp/tunnel/137.44.6.5-137.44.19.200/require;
```

psk.txt

```
137.44.6.5 ThisIsNotActuallyTheKey
```

Server for complex remote

```
remote anonymous {
        proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method pre_shared_key;
                dh_group modp1024;
        }
        generate_policy unique;
        nat_traversal on;
        passive on;
        verify_identifier off;
        lifetime time 60 min;
        exchange_mode main,aggressive;
}
```

Server for complex remote

```
sainfo address 137.44.10.0/25[any] any anonymous {
        pfs_group modp1024;
        lifetime time 20 min;
        encryption_algorithm 3des;
        authentication_algorithm hmac_sha1;
        compression_algorithm deflate;
}
```

psk.txt

```
client-test ThisIsNotActuallyTheKey
```

Server for complex remote

```
remote 137.44.19.200 {
        proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method pre_shared_key;
                dh_group modp1024;
        }
        nat_traversal on;
        my_identifier keyid tag "client-test";
        verify_identifier off;
        lifetime time 60 min;
        exchange_mode aggressive;
}
```

Old Setkey

```
spdadd 137.44.10.0/24 137.44.6.5 any -P out ipsec
    esp/tunnel/137.44.19.200-137.44.6.5/require;

spdadd 137.44.6.5 137.44.10.0/24 any -P in ipsec
    esp/tunnel/137.44.6.5-137.44.19.200/require;
```

New Setkey

```
spdadd 137.44.10.0/24 137.44.6.5 any -P out ipsec
    esp/tunnel/137.44.19.200-137.44.6.5/unique;

spdadd 137.44.6.5 137.44.10.0/24 any -P in ipsec
    esp/tunnel/137.44.6.5-137.44.19.200/unique;
```

The Internet

Slides Available at `http://sucs.org/~eclipse`

Questions?

Any Questions?